

1 What did I do

We tried the sliding window approach before and got the results in Fig. 1. I tried to reproduce these results, but unfortunately, I was not successful. The new results obtained with the sliding window method are given in Fig. 2.

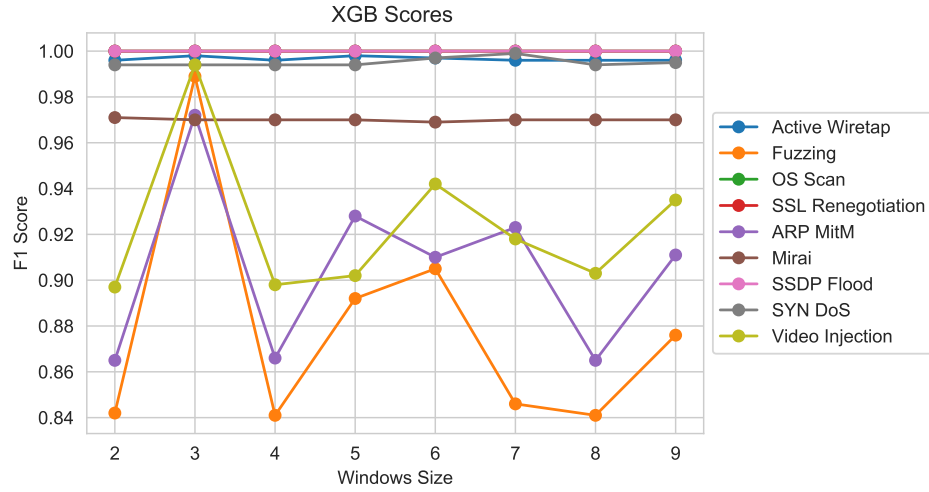


Figure 1: Sliding window results from 3-year report.

The Kitsune dataset was used to obtain these results. Let us explain why we use the Kitsune dataset for this process. We can collect the features we use under 4 main headings. Size, time, flag, and src-dst relationship. The window approach is focused on time and size. MitM attacks can be detected especially through time fluctuations. Kitsune includes 3 MitM attacks. In this context, this dataset is likely to be useful for understanding the effects of window sizes.

The Kitsune dataset was split into two parts according to the sessions. Obtaining different sessions will resist the overfitting problem. The reason why the results presented in Fig. 1 are so high may be that the splitting process was done without paying attention to the session. For both sessions, new features have been introduced with 2-20 sliding windows and expanding window methods (see Fig. 4). In Fig. 3, the results obtained by using the sliding and expanding windows together are given.

In this context, we added the expanding window feature to our feature set and the floating window method for 2,6 and 9 window sizes.

In order to make the work a little simpler, we created a pipeline that extracts features from the pcap files given and performs the labelling process (see Fig. 5). If the data is unlabeled, it creates the tags using the given Wireshark rules. Since the scapy file has difficulty processing large pcap files, it splits pcap files over 100MB and combines the results. In this context, I tried to create a more repeatable and easily understandable method and tool.

We've created a more systematic list of attacks that we're trying to detect. In this context, I chose the



Figure 2: Current sliding window results.

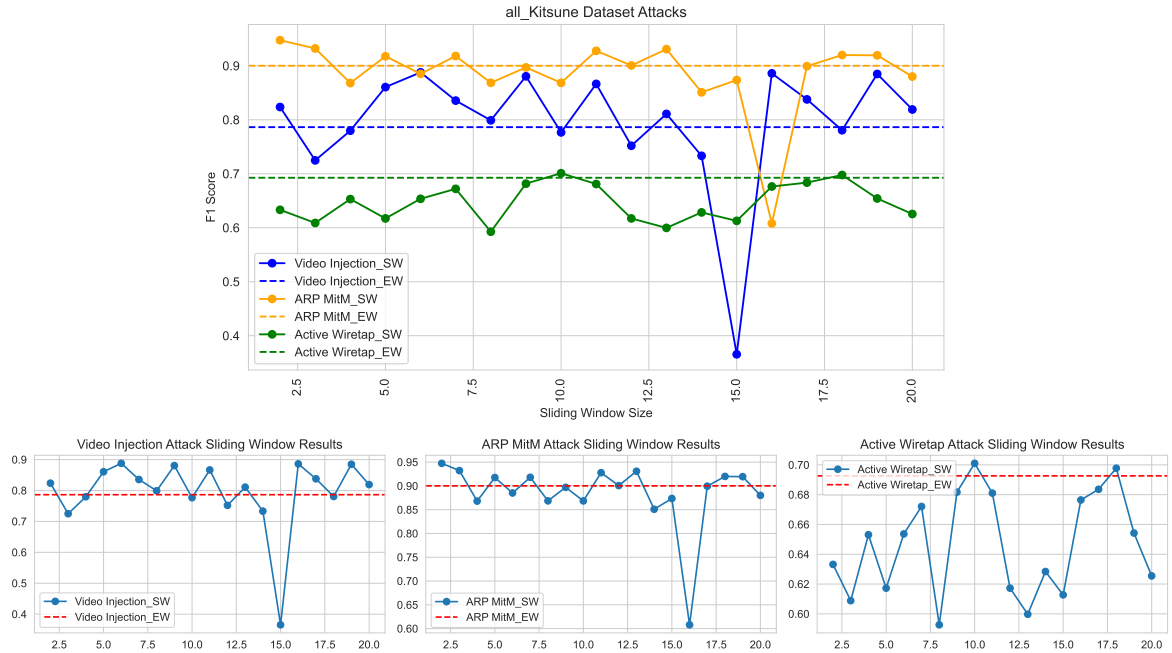



Figure 3: Current sliding window results.

Expanding Window Approach


Packet Number	Packet Size
1	100
2	98
3	95
4	96
5	99
6	102
7	103
8	105
9	105
10	108



The diagram shows a series of blue arrows pointing from the right side of the table towards the left, indicating a window that expands from packet 10 back to packet 1.

Sliding Window Approach

Packet Number	Packet Size
1	100
2	98
3	95
4	96
5	99
6	102
7	103
8	105
9	105
10	108



The diagram shows a series of red arrows pointing from the right side of the table towards the left, indicating a window that slides from packet 10 back to packet 1.

Figure 4: sliding windows and expanding window methods.

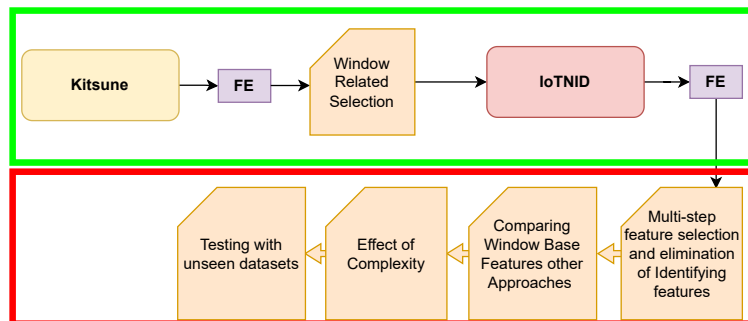


Figure 5: Attack Detection Pipeline

IoTNI dataset as the basis. The reason for this can be explained as follows:

- Containing multiple attacks by different devices in different sessions.
- Using real IoT devices.
- High attack variety. content...

The attack list and attacks equivalents are given in the Fig. 6. Our strategy will be to use this dataset while performing our experiments. In the final stage, we will use the datasets seen for the first time to detect attacks contain by this dataset. Apart from that, we talked about the structure of PhD thesis. The draft of the thesis structure has been sent as an e-mail attachment.

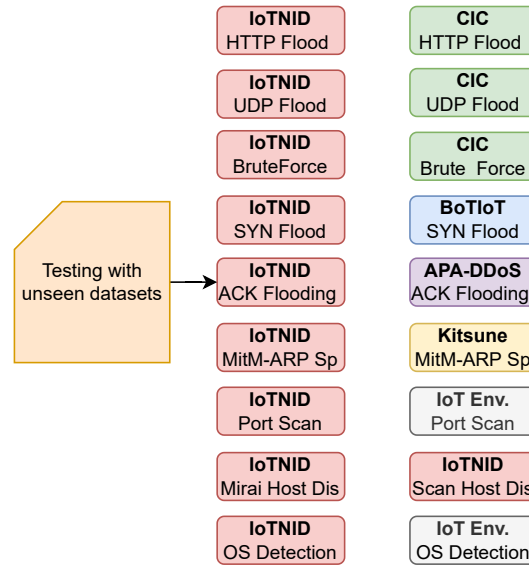


Figure 6: IoTNI Attacks and their equivalents in other datasets

2 What am I doing

We keep doing experiments that expand with the addition of new features and datasets. In this context, I am busy with creating the feature extraction, labelling rules and recoding the experimental steps.

3 What will I do

My near future goal will be to complete the dataset counterparts and feature extraction processes within 1-2 days and to perform the following 4 experiments (see Fig. 5 red frame). I will try to include the use of Transformer and other deep learning methods on my machine learning method list.